

**EXHIBIT 14**  
**Redacted Version of**  
**Document Sought to**  
**be Sealed**

# The Incognito Problem

Chris Palmer (palmer@)

Key Fact:  
Incognito  
Confuses People

## "Incognito" Confuses People

We know from intuition, anecdotes, and now empirically ([Yuxi Wu, et al.](#); see also [Habib, et al.](#)) that the "incognito"/Spy Guy branding, and the complex disclosures (like all complex disclosures), confuse people as to what exact guarantees it offers and does not offer.

Ironically, across all browsers, Chrome's disclosures were the least confusing by a modest amount. But it's still bad.

Id	Date	Text
1	07/22/2018 07:53:36	It'd be good to try to replicate or further validate the study, but I'd be surprised if we got a significantly different result.

WWW 2018, April 23–27, 2018, Lyon, France

Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar<sup>†</sup>, Sascha Fahl<sup>‡</sup>, Blase Ur

**Table 5: Scenarios where participants held misconceptions, shown with the correct answers and percentage of participants who gave incorrect answers. For comparative scenarios, (in)equality symbols denote the correct answer, and we give the sum of all participants answering otherwise.**

Scenario	Answer		% Incorrect	
	Std.	Priv.	Std.	Priv.
<i>Overestimating private mode's privacy protections</i>				
Search queries associated (logged in)	Yes	Yes	1.5	56.3
Bookmarks saved across sessions	Yes	Yes	25.4	46.5
Geolocation can be estimated	Yes	Yes	5.2	40.2
Employer can track browsing	Yes	Yes	1.1	37.0
Better protected from viruses/malware	Std. = Priv.		27.1	
IP address can be collected	Yes	Yes	0.7	25.2
Government can track browsing	Yes	Yes	4.1	22.6
ISP can track browsing	Yes	Yes	3.0	22.0
<i>Underestimating private mode's privacy protections</i>				
Downloaded file in browser's list	Yes	No*	1.3	51.7
Proportion of targeted ads	Std. > Priv.		30.9	
Search queries associated (not logged in)	Yes	No	20.2	30.0

\*Except in Brave's private mode, which does retain download history

**Table 6: Distinguishing scenarios where private mode's impact depends on the browser or context.**

Scenario	% Yes	
	Std.	Priv.
Items in shopping cart saved across sessions	97.8	78.8
Browser extensions active across sessions	98.3	69.1
Forensic expert can reconstruct browsing history	98.7	52.8
Site-specific preferences (e.g., for pop-ups) saved	98.3	31.3

**Table 7: Distribution of responses for comparative scenarios where the impact depends on the browser or context.**

Scenario	% Responses		
	Std. > Priv.	Std. = Priv.	Std. < Priv.
Amount of ads	32.2	64.9	2.9
Page loading speed	24.8	53.6	21.6

( $\chi^2(12) = 38.1, p = .001$ ). In the control condition, 32.4% of participants mistakenly believed downloaded files would still be listed in the browser. A higher proportion of participants in Brave (62.2%,

## This Is Bad

**We are over-promising and under-delivering.**

This is bad for people and reflects badly on our product when/if people do come to understand.

Key Question:  
What Do People  
Use Incognito  
For?

## Why Do People Use Private Modes?

From Wu, et al.:

1. Hide browsing history, especially visits to adult websites;
2. prevent targeted ads and search suggestions;
3. achieve “safer” browsing;
4. Prevent browsers from saving login-related information;
5. avoid cookies;
6. accommodate intentional or unintentional use by others.

Id	Date	Text
1	07/23/2018 13:28:04	what's the motivation here? how does this differ from 2?
2	07/23/2018 13:28:04	This is a list of reasons that people reported to the researchers for why they use private browsing modes. Part of the point of the research is that people don't fully understand the mechanisms.

## Incognito Is Overloaded

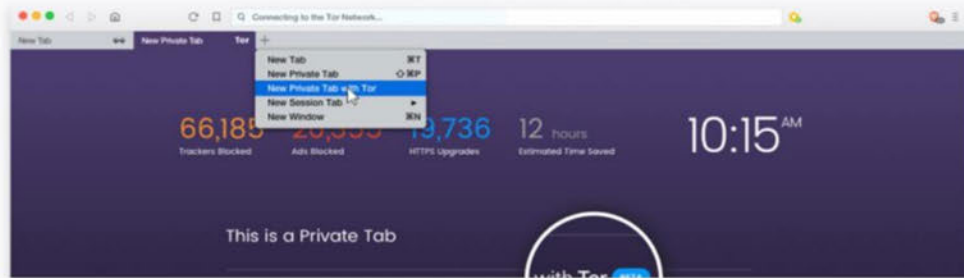
Those 6 reasons are related but different. Perhaps we really need multiple modes (we've already got Guest mode)?

Or more and easier affordances for privacy and control in Settings/elsewhere?

Key Fact: There's  
A Privacy Feature  
Race

# Brave Introduces Beta of Private Tabs with Tor for Enhanced Privacy while Browsing

by Brave | Jun 28, 2018 | Announcements, Features, Privacy



## A Firefox Competitive Advantage

The Tor Project developers said that Project Fusion has the accord of Mozilla's CEO and CTO, which probably means it has a high chance of coming to fruition. However, many issues have to be considered first, such as developing private telemetry, fixing the problem with fingerprinting resistance breaking websites, and so on.

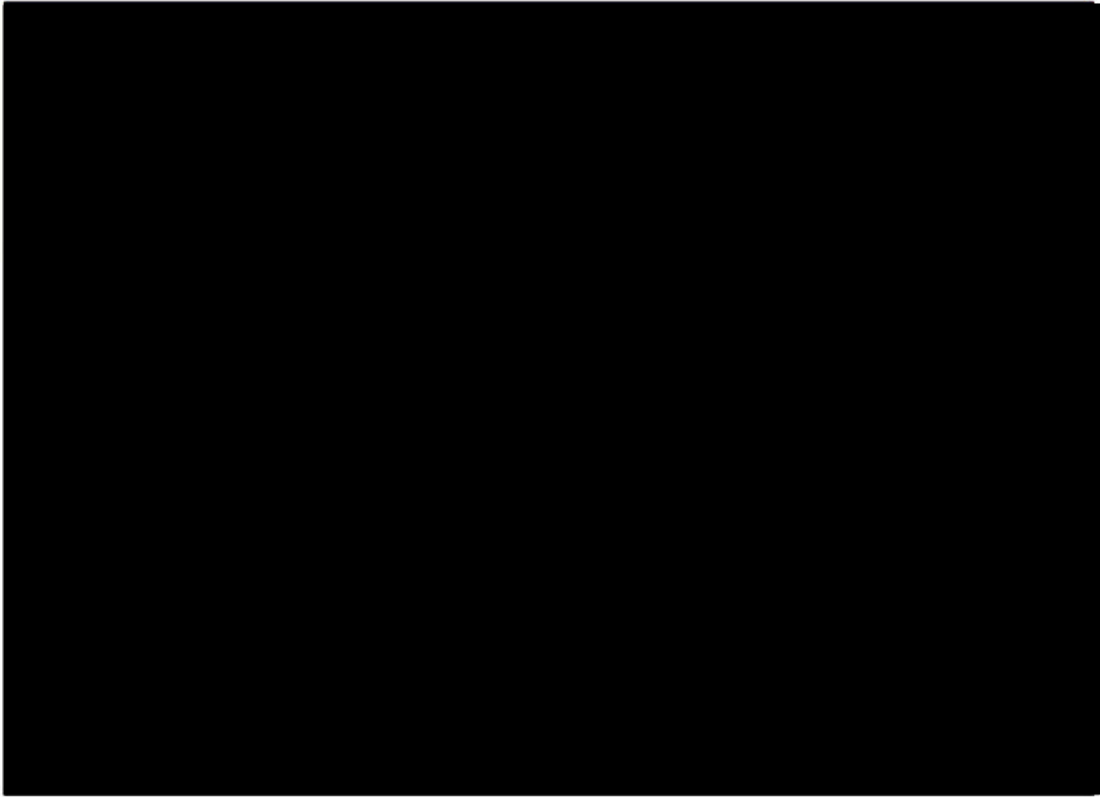
Additionally, Mozilla wants to first standardize the Tor client specification, write conformance tests for it, and open the documentation. All of that means that more people could look at how Tor is implemented in Firefox and see if there are any issues with that implementation.

The main reason why Mozilla would even want to integrate Tor into Firefox is because it could provide its users real private browsing, something that most competitors will not be able to offer. Mozilla has taken an increasingly strong pro-privacy stance in the past few years, and Project Fusion could further boost its pro-privacy image.

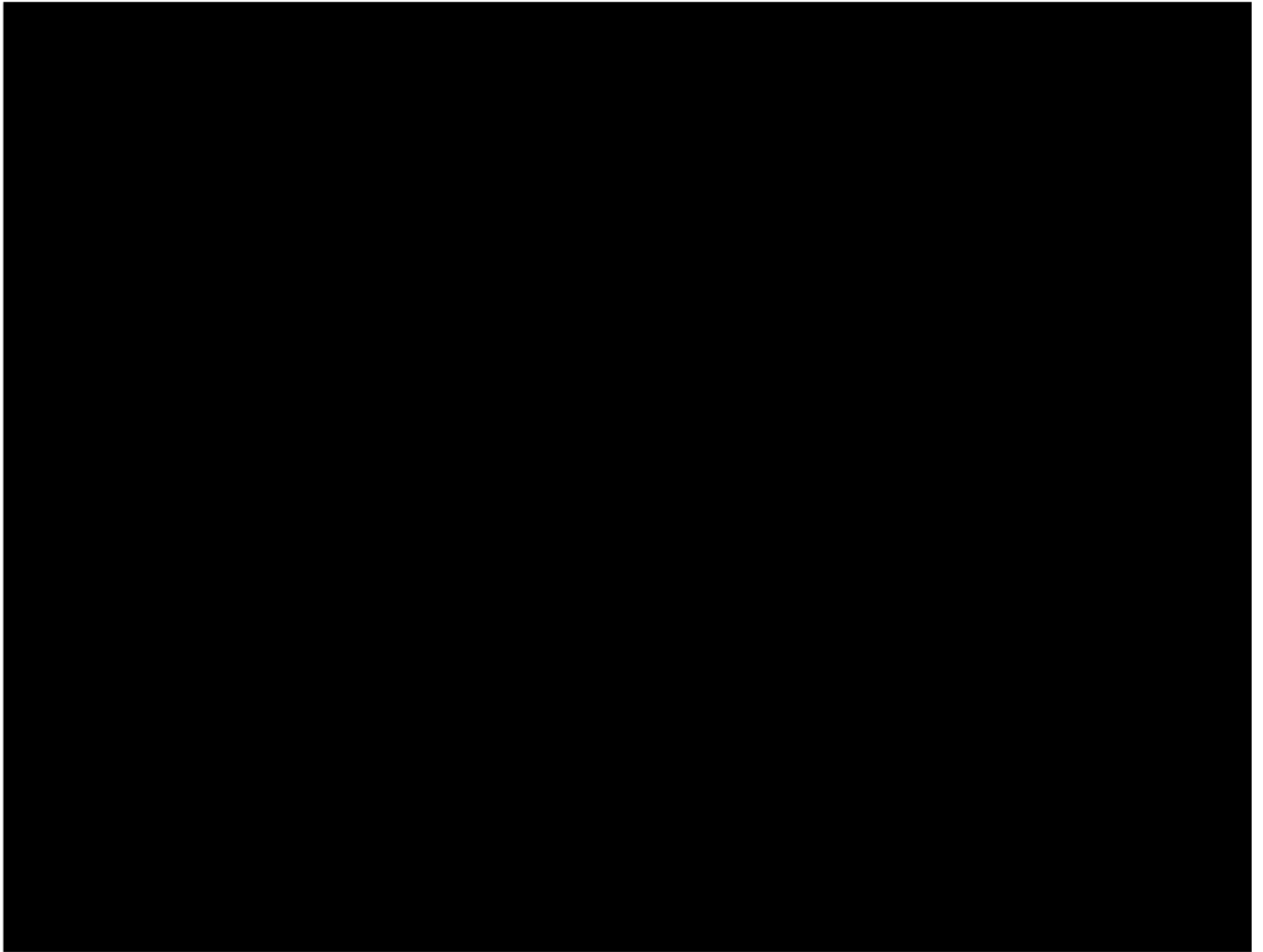
It could also put Firefox in a much more direct contrast with Chrome, a browser developed by Google, which is heavily invested in user tracking in order to serve more targeted ads.

## ITP, ITP2, ITP3

Safari and Mozilla are moving in this area, and we'll need to have some kind of response as well.



Id	Date	Text
1	07/21/2018 14:10:10	Tor is also a cesspool of illegal and distasteful content.





Options

## 1: Ratchet Down Incognito

Use less loaded terms and iconography (e.g. "Temporary Mode", Recycle icon, or whatever).

Simplify the disclosure/disclaimer as a result.

**Benefit: No longer over-promising and under-delivering.**

## 2. Ratchet Up Incognito

We could improve Incognito such that it provides more of what people (both mistakenly, and correctly) expect it does.

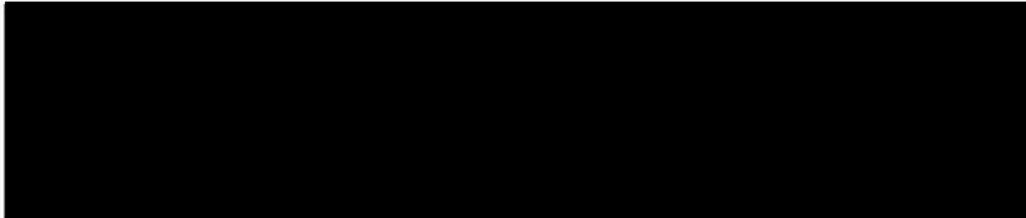
[REDACTED]  
 [REDACTED]  
 [REDACTED]  
 [REDACTED]  
 [REDACTED]  
 [REDACTED]

Id	Date	Text
1	07/23/2018 14:04:19	
1	07/23/2018 14:05:29	
2	07/23/2018 14:05:29	

### 3. Provide Other Privacy/Control Options

Easier access to multi-profile on Desktop?

## 4. Offer Privacy/Circumvention Services



Problem: Google services have a trust perception problem. Would more services help?





## Most VPN Services are Terrible

Short version: I strongly *do not* recommend using any of these providers. You are, of course, free to use whatever you like. My TL;DR advice: Roll your own and use [Algo](#) or [Streisand](#). For messaging & voice, use [Signal](#). For increased anonymity, use [Tor](#) for desktop (though recognize that doing so may actually [put you at greater risk](#)), and [Onion Browser](#) for mobile.

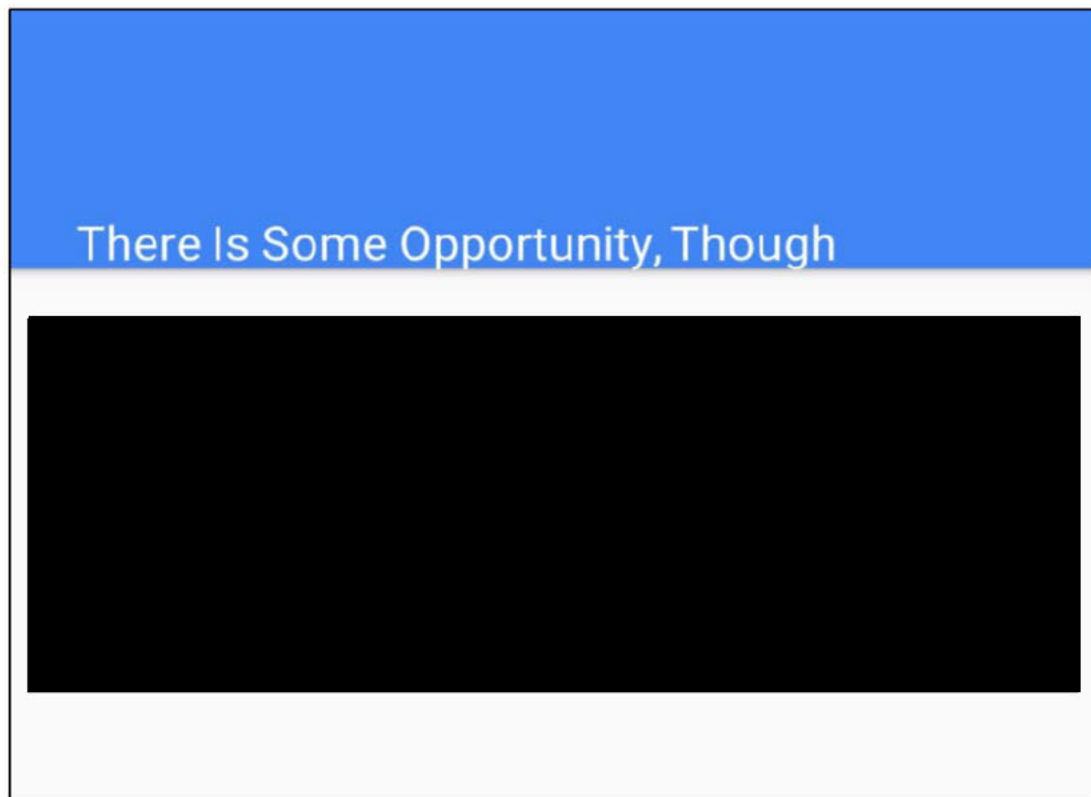
This mini-rant came on the heels of an interesting twitter discussion:  
<https://twitter.com/kennwhite/status/591074055018582016>

Again I strongly *do not* recommend using any of these providers.

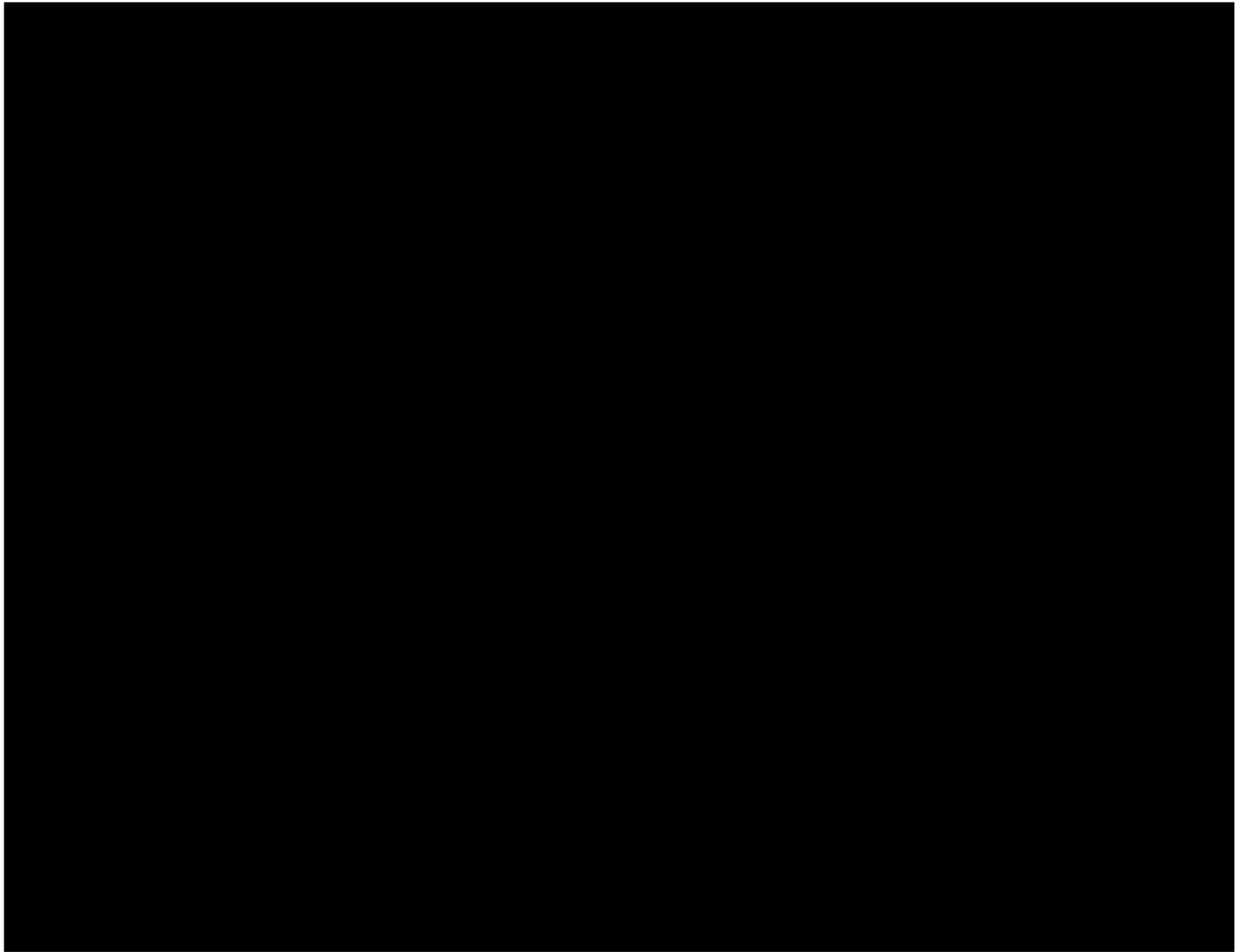
Provider / known "Secret" Key

```
Astril / way2stars
EarthVPN / earthvpn
GFWVPN / gfwvpn
GoldenFrog / thisisourkey
IBVPN / ibVPNsharedPSK!
IPVanish / ipvanish
NordVPN / nordvpn
PrivateInternetAccess (PIA) / mysafety
PureVPN / 12345678
SlickVPN / gogoVPN
TorGuard / torguard
TigerVPN / tigerVPN
```

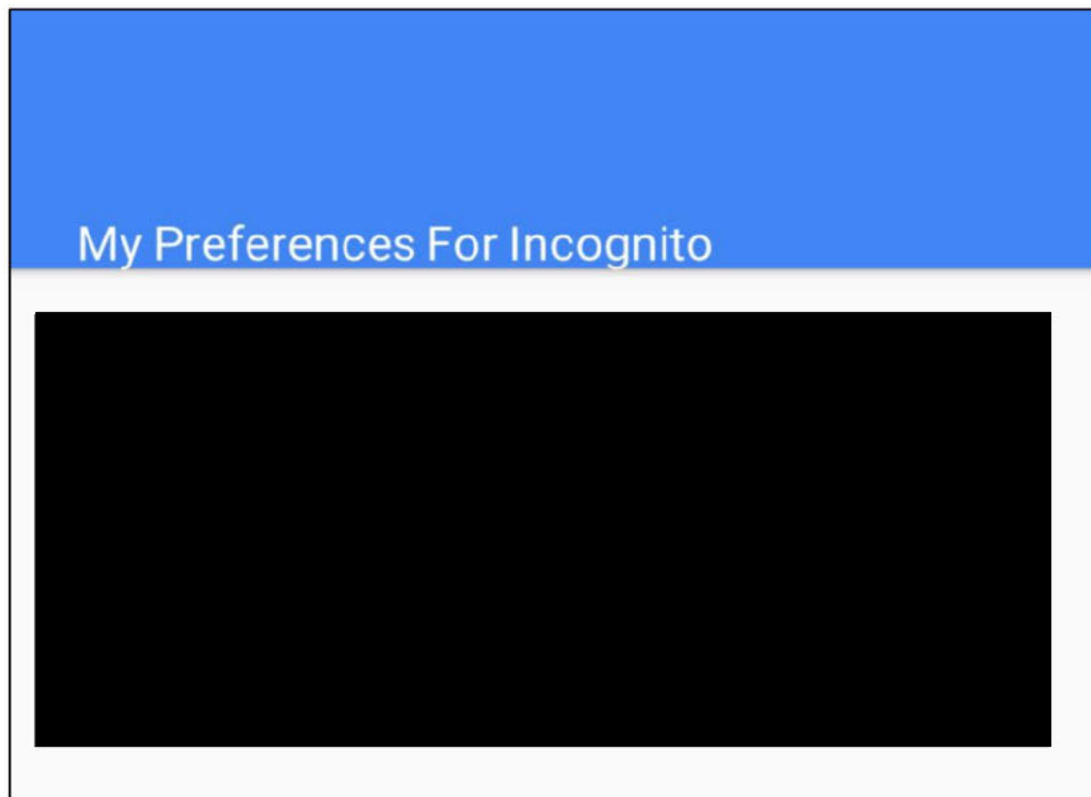
source: <https://gist.github.com/kennwhite/1f3bc4d889b02b35d8aa>



Key Question:  
How Much  
Breakage Will  
People Tolerate?



Conclusion:  
Options, But No  
Single Clear Path



Id	Date	Text
1	07/21/2018 15:50:53	
3	07/22/2018 08:00:43	
2	07/23/2018 12:54:42	
3	07/23/2018 12:54:42	

## Additional Useful Efforts

